CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A processor for encrypting and decrypting data comprising:

a control device that receives a data word for encryption or decryption ~~is connected to at least one encryption/decryption means via at least one communication means, wherein~~, the control device ~~comprises~~ comprising:

a memory that temporarily stores an initial key, and

at least one external key input that receives ~~an~~ the initial key from a source ~~other than the key generation means, and~~;

~~at least one round key generation means~~ a round key generator connected to the control device via at least one further communication ~~means~~ device, wherein the round key ~~generation means~~ generator receives ~~a~~ the data word from the control device for calculating at least one round key and transfers the at least one round key to the memory of the ~~storage~~ control device; and ~~wherein the~~

at least one encryption/decryption device ~~means comprises~~ comprising:

at least one external data input ~~for receiving the~~ that receives external data,

an input ~~for receiving~~ that receives the at least one round key from the memory of the control device, and

at least one external data output ~~for outputting~~ that outputs data processed with the at least one round key, ~~and~~

wherein the at least one encryption/decryption ~~means~~ device and the ~~at least one~~ round key ~~generation means~~ generator communicate solely via the control device, and the control device transmits intermediate results to the round key generator to perform recursive calculation of the at least one round key.

2. (Currently Amended) The processor of claim 1, wherein the at least one communication ~~means~~ device further comprises:

~~at least one~~ first and second request ~~line~~ lines;

~~at least one~~ first and second release ~~line~~ lines; and

~~at least one~~ first and second data lines ~~and the at least one further communication means comprises at least one further request line, at least one further release line and at least one further data line~~.

3. (Currently Amended) The processor of ~~claim 1~~ claim 2, ~~characterized in that~~ wherein the first and second request lines, the first and second release lines, and the first and second data lines ~~at least one request line, the at least one release line~~

~~and the at least one data line and the at least one further request line, the at least one further release line and the at least one further data line~~ at least partially use ~~the same~~ a single physical path.

4. (Currently Amended) The processor of claim 1, wherein the at least one round key is temporarily stored in the memory of the control device.

5. (Currently Amended) The processor of claim 1, wherein the at least one round key ~~from the memory of the control device~~ is accessed using a rotating pointer.

6. (Currently Amended) The processor of claim 1, wherein the communication between the control device and the at least one encryption/decryption ~~means~~ device and between the control device and the ~~at least one~~ round key ~~generation means~~ generator is accomplished using at least one handshake protocol.

7. (Currently Amended) The processor of claim 1, wherein the operation of the control device, of the at least one encryption/decryption ~~means~~ device, and of the ~~at least one~~ round key ~~generation means~~ generator are asynchronous with respect to one another.

8. (Currently Amended) The processor of claim 1, wherein the round key ~~generation means~~ generator is adapted to perform a dummy operation.

9. (Currently Amended) The processor of claim 1, wherein a time between the calculating of the at least one round key by the round key ~~generation means~~ generator and the processing of the external data using the at least one round key is variable.

10. (Currently Amended) The processor of claim 1, wherein the processor is an ~~AES~~ Advanced Encryption Standard (AES) coprocessor.

11. (Currently Amended) A method of encrypting and/or decrypting data using a processor comprising:

~~a)~~ reading at least one initial key ~~is read~~ into a control device, wherein the at least one initial key is obtained from a source other than a round key generator ~~generation means,~~;

~~b)~~ reading external data ~~are read~~ into at least one encryption/decryption ~~means~~[[,]] device;

~~c)~~ reading at least one data word needed to calculate at least one round key ~~is read~~ from at least one storage ~~means~~ device of the control device; ~~and transferred~~

transferring the at least one data word to ~~at least one~~ the round key generator ~~generation means,~~;

~~d)~~ calculating at least one round key ~~is calculated~~ recursively on the basis of the at least one data word by ~~means of~~ using the ~~at least one~~ round key generator ~~generation means,~~;

~~transferred~~ transferring the calculated key to the control device; and

~~stored~~ storing the transferred key in the at least one storage ~~means~~[[,]] device;

~~e)~~ transferring the at least one round key ~~is transferred~~ from the at least one storage ~~means~~ device to the at least one encryption/decryption ~~means~~[[,]] device;

~~f)~~ processing the external data ~~are processed~~ by ~~means of~~ using the at least one encryption/decryption ~~means~~ device, using the at least one round key, and using the processed data are made available at at least one external data output[[,]]; and

~~g) steps b) to f) are repeated~~ repeating the method as often as necessary to encrypt or decrypt a set of external data.

wherein the control device transmits intermediate results to the round key generator to perform recursive calculation of the at least one round key.

12. (Currently Amended) The method of claim 11, wherein ~~the~~ communication between the control device ~~with~~ and the at least one encryption/decryption ~~means~~ device, and between the control device and the ~~at least one~~ round key ~~generation means~~ generator is accomplished using at least one handshake protocol.

13. (Currently Amended) The method of claim 11, wherein the operation of the control device, of the at least one encryption/decryption ~~means~~ device, and of the ~~at least one~~ round key ~~generation means~~ generator are asynchronous with respect to one another.

14. (Currently Amended) The method of claim 11, wherein the at least one round key ~~from the memory of the control device~~ is accessed using a rotating pointer.

15. (Currently Amended) The method of claim 11, further comprising:

performing a dummy operation using the round key ~~generation means~~ generator.

16. (Currently Amended) The method of claim 11, wherein a time between the calculating of the at least one round key by the round key ~~generation means~~ generator and the processing of the data using the at least one round key is variable.

17. (Currently Amended) The method of claim 11, wherein the processor is an ~~AES~~ Advanced Encryption Standard (AES) coprocessor.